IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. ARIEL MANUEL FRIEDLER, Defendant.	Criminal No. 1:14-cr-181 Count 1: 18 U.S.C. § 371 Conspiracy to Access a Protected Computer Without Authorization Forfeiture Notice

CRIMINAL INFORMATION

COUNT ONE

(Conspiracy to Access a Protected Computer without Authorization)

THE UNITED STATES ATTORNEY CHARGES THAT:

1. Symplicity Corporation ("Symplicity") was a corporation headquartered in Arlington, Virginia, in the Eastern District of Virginia. Symplicity offered higher education software products for colleges and universities, federal government systems development for communications management products used by the United States government, including the White House and members of Congress, and secure managed hosting. Symplicity also sold a Student Conduct Records Management ("SCRM") system allowing colleges and universities to track student disciplinary records. Its SCRM product was called "Advocate" or "JAMS."

2. Defendant ARIEL MANUEL FRIEDLER was the Chief Executive Officer and president of Symplicity.

3. A.D. was Symplicity's Chief Technology Officer responsible for software development and systems administration.

4. M.K. was Symplicity's Director of Higher Education Product Sales.

5. Company A was headquartered in Texas, and competed against Symplicity in the SCRM business.

6. Maxient LLC ("Maxient") was headquartered in Charlottesville, Virginia, and also competed against Symplicity in the SCRM business. Maxient's product was called "Conduct Manager."

7. Companies providing SCRM systems derive their competitive edge from the design and features of the system, which they consider proprietary and confidential. As a result, they require clients or potential clients to sign agreements with non-disclosure provisions, and frequently file open records requests to learn more about their competitors.

8. From on or about October 17, 2007, and continuing thereafter until on or about October 27, 2011, in the Eastern District of Virginia and elsewhere, defendant ARIEL MANUEL FRIEDLER, A.D., and M.K., each knowingly and intentionally conspired and agreed together and with each other, and with others, to commit an offense against the United States, that is, to knowingly and intentionally access a computer without authorization, and thereby to obtain information from a protected computer, and the offense was committed for purposes of commercial advantage and private financial gain, in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B)(i).

MANNER AND MEANS OF THE CONSPIRACY

It was a part of the conspiracy that:

9. Defendant ARIEL MANUEL FRIEDLER led the conspiracy, organized the intrusions, recruited employees to decrypt encrypted passwords, and used anonymizing software in preparation for intrusions. After accessing sensitive and valuable business information from Symplicity's competitors, FRIEDLER copied, saved, and shared this information with co-

conspirators and other employees to inform Symplicity's software development and sales strategy.

10. A.D. provided technical assistance to defendant ARIEL MANUEL FRIEDLER for the unauthorized accesses. A.D. helped recover and decrypt passwords of former Symplicity clients and tested anonymizing software before unauthorized accesses into a competitor's computer.

OVERT ACTS

In furtherance of the conspiracy and to effect the objects of the conspiracy, the following overt acts, among others, were committed in the Eastern District of Virginia and elsewhere:

The Unauthorized Access into Company A

11. On or about October 17, 2007, defendant ARIEL MANUEL FRIEDLER gained access to the protected computer systems of Company A without authorization to obtain confidential and proprietary business information from a competitor. Specifically, defendant FRIEDLER, without authorization, accessed and copied Company A's confidential and proprietary business information related to the company's client names and information on features into a comprehensive spreadsheet (the "Company A Spreadsheet").

12. Also on or about October 17, 2007, defendant ARIEL MANUEL FRIEDLER sent multiple emails to a cooperating witness, CW-1, containing a list of Company A's current clients, a list of potential clients that had asked Company A for prices, and the Company A Spreadsheet. FRIEDLER then instructed CW-1, "for [Company A] client list who are also symp customers please send a persaonlzied [sic] email, ccing career center and also telling them we know they are a[Company A] client and we can do a lot more for them."

The Unauthorized Accesses into Maxient LLC

13. From on or about January 22, 2010 through on or about January 23, 2010, defendant ARIEL MANUEL FRIEDLER and A.D. exchanged the following messages:

FRIEDLER:	Do u have tor working?
A.D.:	For?
FRIEDLER:	I can't get firefox to not show proxy error when I turn tor on. Was wondering if problem with snow
A.D.:	But all other browsers are fine? That's bizarre. Maybe try clearing cache etc? Ff works fine for me on all my snow machines - 2 havkintosh and 1 MacBook.
FRIEDLER:	sorry -- i meant when using TOR..trying to get into a competitors shit

TOR is a free software tool that allows users to hide their IP address and use the Internet anonymously.

14. On or about January 24, 2010, defendant ARIEL MANUEL FRIEDLER unsuccessfully attempted to log in to Maxient's servers twice without authorization using the login credentials for "Employee A" of "University No. 1."

15. Between at least on or about May 28, 2010 to at least on or about September 11, 2010, Symplicity lost customers to Maxient on the SCRM product line. For example, on or about September 8, 2010, after Maxient won another bid, defendant ARIEL MANUEL FRIEDLER emailed company employees, including A.D. and M.K. that "we need to make advocate a website look and feel that is the point and why we lost [a university client] to maxient today. they said maxient feels like a website and for users that use it a few times a year that is what they are seeking.... we are bleeding advocate alok -- we have lost close to a dozen this year."

16. On or about September 13, 2010, after losing another client to Maxient, defendant ARIEL MANUEL FRIEDLER asked a Symplicity employee for email addresses and the

encrypted passwords of a former customer, "University No. 1." FRIEDLER told A.D.: "want to see if we can use old client who used us to get into maxient -- ill do it from somewhere else... there are some online tools that give u reverse if they are common words."

17. A.D. then used a reverse-lookup website to decrypt passwords for employees of former client "University No. 2" and forwarded them to defendant ARIEL MANUEL FRIEDLER.

18. Upon receiving the passwords from A.D., defendant ARIEL MANUEL FRIEDLER asked for the decrypted passwords for "University No. 3" employees, stating: "desperate times calls for desperate measures." A.D. complied, sending to FRIEDLER the decrypted passwords, including that of "Employee B."

19. Later that evening, defendant ARIEL MANUEL FRIEDLER and A.D. had the following exchange:

FRIEDLER:	what ip lookup do u get for ip 208.53.142.37[?]
A.D.:	Some weird tor address - guessing that's w the onion routing thing on
FRIEDLER:	cool -- so masked

20. Defendant ARIEL MANUEL FRIEDLER then logged into Maxient's servers using login credentials for "Employee B" from "University No. 3."

21. While logged into Maxient's servers as "Employee B," defendant ARIEL MANUEL FRIEDLER reviewed Maxient's confidential and proprietary product design and manuals, and copied-and-pasted key proprietary and confidential information into a 110-page document and saved it as maxient.docx (the "Maxient Document") on a computer. The Maxient Document contained detailed information about Maxient's new and key features, planned upgrades, layout of the software, and key screen shots.

22. Two days after the unauthorized access, on or about September 15, 2010, defendant ARIEL MANUEL FRIEDLER and M.K. discussed which features to add to Symplicity's SCRM product, in an email with the subject line "Maxient features to add."

23. Later that day, defendant ARIEL MANUEL FRIEDLER instructed M.K. not to reveal the unauthorized access: "hey until dust settles for me doent [sic] say anythign [sic] ab out seeing competitors shit to anyone but alok or brian which know not worth it in a month or two sure." M.K. responded "ok."

24. On or about September 26, 2010, M.K. asked defendant ARIEL MANUEL FRIEDLER in an email with the subject line: "Re: Maxient features to add" if there was "[a]nything else cool that you remember that they have that we don't?" FRIEDLER responded: "personal watch list -- where each user can set up pwn tracked set of students and system emails them whenever something comes up with them."

25. After losing more SCRM clients to Maxient, on or about January 10, 2011, defendant ARIEL MANUEL FRIEDLER and A.D. engaged in the following exchange:

FRIEDLER:	hey – remember that those reverse ahshes [sic] u did a while ago =- i dont want to login again, but deleting that db and want to have just in case do u have it and can u resend
A.D.:	im not entirely sure what we're talking about - the super h@ckery?
FRIEDLER:	y
A.D.:	did i email it?
FRIEDLER:	.uy
A.D.:	then i'd have it - what was the rough date range
FRIEDLER:	oy search for [Employee B] that should pull it up
A.D.:	n
FRIEDLER:	[University No. 3] date range then sept 7-13

FRIEDLER and A.D. then discussed how to decrypt additional passwords of former clients, and A.D. sent to FRIEDLER the chart containing the usernames and decrypted passwords of employees at former client "University No. 3."

26. On or about February 8, 2011, defendant ARIEL MANUEL FRIEDLER emailed to A.D. and M.K. a screen shot from a key Maxient feature.

27. On or about August 2, 2011, defendant ARIEL MANUEL FRIEDLER and M.K. in an online chat discussed customers' preference for Maxient:

FRIEDLER:	its a rough situation
M.K.:	whole world is full of bafoons...
FRIEDLER:	i need to login... and see if they changed it or something only explanation

28. On or about August 17, 2011, defendant ARIEL MANUEL FRIEDLER, after obtaining decrypted passwords from A.D., logged into the Maxient server using the login credentials of "Employee C," an employee at Symplicity's former client "University No. 1." FRIEDLER also attempted to login using the username and password for "Employee A," also an employee of Symplicity's former client "University No. 1."

29. A few hours after defendant ARIEL MANUEL FRIEDLER accessed Maxient's systems without authorization on or about August 17, 2011, M.K. sent emails containing ideas and talking points for how to distinguish the Symplicity SCRM product from Maxient's to other employees.

(All in violation of Title 18, United States Code, Section 371)

NOTICE OF FORFEITURE

Pursuant to Rule 32.2(a), the defendant is notified that, if convicted of Count One above, he shall forfeit to the United States of America, pursuant to Title 18, United States Code, Sections 982(a)(2)(B), 981(a)(1)(C), and 1030(i), and Title 28, United States Code, Section 2461(c), the defendant's interest in any personal property that was used or intended to be used to commit or facilitate the commission of such violations, and any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violations.

If any of the property described above as being forfeitable pursuant to Title 18, United States Code, Section 981(a)(1)(C); Title 28, United States Code, Section 2461(c); Title 18, United States Code, Section 982(a)(2)(B); and Title 18, United States Code, Section 1030(i) as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States of America, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c); Title 18,

United States Code, Section 982(b)(1), and Title 18, United States Code, Section 1030(i)(2), to seek forfeiture of substitute assets.

(All pursuant to 18 U.S.C. §§ 981(a)(1)(C); 982(a)(2)(B), and 1030(i); 21 U.S.C. § 853(p); and 28 U.S.C. § 2461(c); Rule 32.2(a), Federal Rules of Criminal Procedure)

DANA J. BOENTE
UNITED STATES ATTORNEY

Alexander T.H. Nguyen
Assistant United States Attorney

Peter V. Roman
Trial Attorney, U.S. Department of Justice
Computer Crime & Intellectual Property Section